View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 34, 82–94 (1990)

Quadratische Ordnungen mit großer Klassenzahl

FRANZ HALTER-KOCH

Institut für Mathematik, Karl-Franzens-Universität, Halbärthgasse 1/I, A-8010 Graz, Austria

Communicated by P. Roquette

Received January 23, 1989

An estimate for the class number of certain quadratic orders from below is given. The method is elementary and applies for imaginary and real quadratic orders of Richaud–Degert and similar types, which usually have large class numbers. © 1990 Academic Press, Inc.

EINLEITUNG

In den letzten Jahren erschien eine Reihe von Arbeiten über die Klassenzahlen spezieller Typen reell-quadratischer Zahlkörper. Ziel dieser Untersuchungen waren elementare Mehrklassigkeitskriterien für Primdiskriminanten, aber auch Abschätzungen der Klassenzahl nach unten. Methodisch standen diese Untersuchungen entweder im Zusammenhang mit Kettenbrüchen (z. B. in [9, 6, 1, 2, 15]) oder im Zusammenhang mit quadratischen diophantischen Gleichungen (z. B. in [5, 16, 17, 11–13]).

In der vorliegenden Note beweise ich mit elementaren Methoden eine für alle quadratischen Ordnungen gültige Klassenzahlabschätzung nach unten. Diese ist für imaginär-quadratische Ordnungen unmittelbar anwendbar, für reell-quadratische Ordnungen nur dann, wenn man Informationen über die Normen der reduzierten Hauptideale besitzt, also insbesondere dann, wenn man die Kettenbruchentwicklung der zugehörigen Basiszahl kennt. Für Ordnungen vom Richaud–Degert'schen und ähnlichem Typ erhält man damit erhebliche Verallgemeinerungen und Verschärfungen der bisher bekannten Resultate.

In Sektion 1 stelle ich die im folgenden benötigten Hilfsmittel aus der Idealtherie der quadratischen Ordnungen und der Theorie der Kettenbrüche zusammen. In Sektion 2 beweise ich einen allgemeinen Satz über Klassenzahlabschätzungen nach unten und diskutiere erste Anwendungen. In den Sektionen 3 und 4 betrachte ich Ordnungen vom Richaud–Degert'schen Typ.

0022-314X/90 $3.00

Copyright © 1990 by Academic Press, Inc.
All rights of reproduction in any form reserved.

Im Gegensatz zur bisherigen Literatur formuliere ich alle Resultate nicht nur für die Hauptordnung (wenn auch dieser das meiste Interesse gilt). Das kostet nur unwesentlich mehr Mühe, erspart Voraussetzungen über quadratische Faktoren in der Diskriminante und bringt eine etwas größere Allgemeinheit der Resultate.

1. Ideale in quadratischen Ordnungen, quadratische Irrationalitäten und Kettenbrüche

Für die Beweise der in diesem Paragraphen referierten Tatsachen vergleiche man [4, 7, 8, 1, 15], für die Kettenbrüche [14]. Manche der dort nur für die Hauptordnung formulierten und bewiesenen Resultate bleiben im allgemeinen Fall fast wörtlich gültig.

Eine ganze Zahl D heiße *Diskriminante*, wenn D kein Quadrat und entweder $D \equiv 0 \bmod 4$ oder $D \equiv 1 \bmod 4$ ist; sei im folgenden stets D eine Diskriminante. Ich setze

$$\omega_D = \begin{cases} \frac{1}{2} \cdot \sqrt{D}, & \text{falls } D \equiv 0 \bmod 4, \\ \frac{1}{2} \cdot (1 + \sqrt{D}), & \text{falls } D \equiv 1 \bmod 4, \end{cases}$$

und

$$\mathcal{R}_D = \mathbf{Z} \oplus \mathbf{Z} \cdot \omega_D.$$

$\mathcal{R}_D$ ist eine Ordnung im quadratischen Zahlkörper $\mathbf{Q}(\sqrt{D})$; ist D_0 die Diskriminante von $\mathbf{Q}(\sqrt{D})$, so ist $D = D_0 f^2$ mit $f \in \mathbf{N}$, und man nennt D_0 die zu D gehörige *Fundamentaldiskriminante*, $\mathcal{R}_D$ die *quadratische Ordnung mit Diskriminante D* und f den *Führer* von $\mathcal{R}_D$. Jedes $\xi \in \mathcal{R}_D$ hat eine eindeutige Darstellung in der Form

$$\xi = \frac{b + e\sqrt{D}}{2}$$

mit $b, e \in \mathbf{Z}$, $b \equiv eD \bmod 2$.

Jedes Ideal $\mathcal{J} \neq (0)$ von $\mathcal{R}_D$ ist ein freier $\mathbf{Z}$-Modul vom Rang 2 und hat daher die Form

$$\mathcal{J} = \mathbf{Z} \cdot a \oplus \mathbf{Z} \cdot \frac{b + e\sqrt{D}}{2} \quad \text{mit} \qquad (*)$$
$$a, b, e \in \mathbf{Z},\ a > 0,\ e > 0,\ b \equiv dD \bmod 2.$$

Ist umgekehrt ein freier $\mathbf{Z}$-Modul $\mathcal{J} \subset \mathcal{R}_D$ durch $(*)$ gegeben, so ist $\mathcal{J}$ genau dann ein Ideal von $\mathcal{R}_D$, wenn

$$e \mid a, \qquad 2e \mid (eD - b) \qquad \text{und} \qquad 4ae \mid (b^2 - De^2);$$

dann ist

$$\mathcal{N}(\mathcal{J}) = (\mathcal{R}_D : \mathcal{J}) = ae,$$

und $e^{-1} \cdot \mathcal{J}$ ist ebenfalls ein Ideal von $\mathcal{R}_D$. Ist $e = 1$, so nennt man $\mathcal{J}$ *primitiv*; dann ist $m^{-1}\mathcal{J}$ für kein $m \in \mathbf{N}$ mit $m \geqslant 2$ ein Ideal von $\mathcal{R}_D$.

Sei nun $\mathcal{J} = \mathbf{Z} \cdot a \oplus \mathbf{Z} \cdot (b + \sqrt{D})/2$ ein primitives Ideal von $\mathcal{R}_D$ ($a, b \in \mathbf{Z}$, $a > 0$, $b^2 \equiv D \bmod 4a$). $\mathcal{J}$ heißt *regulär*, wenn

$$\left(a, b, \frac{b^2 - D}{4a}\right) = 1;$$

ist $\mathcal{J}$ regulär, so ist $\mathcal{J}$ invertierbar, und für das zu $\mathcal{J}$ konjugierte Ideal $\mathcal{J}' = \mathbf{Z} \cdot a \oplus \mathbf{Z} \cdot (-b + \sqrt{D})/2$ gilt:

$$\mathcal{J} \cdot \mathcal{J}' = a \cdot \mathcal{R}_D.$$

Zwei invertierbare $\mathcal{R}_D$-Ideale $\mathcal{J}_1$, $\mathcal{J}_2$ heißen *äquivalent*, wenn es $\beta_1, \beta_2 \in \mathcal{R}_D \setminus \{0\}$ gibt mit $\beta_1 \mathcal{J}_1 = \beta_2 \mathcal{J}_2$. Die Äquivalenzklassen invertierbarer $\mathcal{R}_D$-Ideale bilden bezüglich der Multiplikation eine zu $\operatorname{Pic} \mathcal{R}_D$ isomorphe abelsche Gruppe $\mathcal{C}_D$ der Ordnung h_D.

Ein primitives Ideal $\mathcal{J}$ von $\mathcal{R}_D$ heißt zum Führer f von $\mathcal{R}_D$ prim, wenn $(\mathcal{N}(\mathcal{J}), f) = 1$. Jedes zu f prime primitive Ideal ist regulär, also invertierbar, und in jeder Klasse von $\mathcal{C}_D$ gibt es zu f prime primitive Ideale.

Im Falle $D < 0$ enthält jede Klasse von $\mathcal{C}_D$ ein Ideal $\mathcal{J}$ mit $\mathcal{N}(\mathcal{J}) < \sqrt{-D/3}$, und für jedes primitive Hauptideal $\mathcal{J} = (b + e\sqrt{D})/2 \cdot \mathcal{R}_D \neq \mathcal{R}_D$ (mit $b, e \in \mathbf{Z}$, $b \equiv eD \bmod 2$, $(b, e) \mid (2, D)$) gilt

$$\mathcal{N}(\mathcal{J}) = \frac{b^2 - e^2 D}{4} \geqslant \begin{cases} (1 - D)/4, & \text{falls } D \equiv 1 \bmod 4, \\ (-D/4), & \text{falls } D \equiv 0 \bmod 4. \end{cases}$$

Sei von nun an $D > 0$.

Eine reelle Zahl ξ heißt *quadratische Irrationalität* mit Diskriminante D, wenn

$$\xi = \frac{b + \sqrt{D}}{2a}$$

mit $a, b \in \mathbf{Z}$, $a > 0$,

$$4a \mid (b^2 - D) \qquad \text{und} \qquad \left(a, b, \frac{b^2 - D}{4a}\right) = 1;$$

a und b sind durch ξ eindeutig bestimmt. Ich setze

$$\theta(\xi) = \mathbf{Z} \cdot a \oplus \mathbf{Z} \cdot \frac{b + \sqrt{D}}{2};$$

dann ist $\theta(\xi)$ ein reguläres Ideal von $\mathscr{R}_D$ mit $\mathscr{N}\theta(\xi) = a$, und jedes reguläre Ideal von $\mathscr{R}_D$ ist von dieser Gestalt.

Zwei quadratische Irrationalitäten (derselben Diskriminante D) ξ, η heißen *äquivalent*, wenn

$$\eta = \frac{u\xi + v}{\omega\xi + z}.$$

mit $u, v, w, z \in \mathbf{Z}$, $uz - vw = 1$; ξ und η sind genau dann äquivalent, wenn $\theta(\xi)$ und $\theta(\eta)$ äquivalente $\mathscr{R}_D$-Ideale sind. Somit induziert θ eine Bijektion von der Menge der Äquivalenzklassen quadratischer Irrationalitäten mit fester Diskriminante D auf $\mathscr{C}_D$.

Eine quadratische Irrationalität ξ heißt *reduziert*, wenn

$$\xi > 1, \qquad -1 < \xi' < 0;$$

dabei bezeichne ξ' stets die zu ξ *konjugierte* quadratische Irrationalität. Ein reguläres Ideal $\mathscr{J}$ von $\mathscr{R}_D$ heißt *reduziert*, wenn es eine reduzierte quadratische Irrationalität ξ mit $\mathscr{J} = \theta(\xi)$ gibt.

θ ist eine Bijektion von der Menge der reduzierten quadratischen Irrationalitäten der Diskriminante D auf die Menge der reduzierten Ideale von $\mathscr{R}_D$.

Ein reguläres Ideal $\mathscr{J}$ von $\mathscr{R}_D$ mit $\mathscr{N}(\mathscr{J}) < \frac{1}{2}\sqrt{D}$ ist reduziert, und für jedes reduzierte Ideal $\mathscr{J}$ von $\mathscr{R}_D$ ist $\mathscr{N}(\mathscr{J}) < \sqrt{D}$. In jeder Klasse von $\mathscr{C}_D$ gibt es reduzierte Ideale, und daher induziert θ eine Bijektion von der Menge der Äquivalenzklassen reduzierter quadratischer Irrationalitäten der Diskriminante D auf $\mathscr{C}_D$.

Eine reelle Zahl ξ_0 ist genau dann eine reduzierte quadratische Irrationalität, wenn ξ_0 eine rein-periodische Kettenbruchentwicklung besitzt. Ist ξ eine beliebige quadratische Irrationalität der Diskriminante D und hat die Kettenbruchentwicklung von ξ die Form

$$\xi = [b_0, \ldots, b_{k-1}, \overline{b_k, \ldots, b_{k+l-1}}]$$

mit minimalem $l = \lambda(\xi)$ (Länge einer *primitiven Periode*), so sind die l reduzierten quadratischen Irrationalitäten

$$\xi_\nu = [\overline{b_{k+\nu}, \ldots, b_{k+l-1}, b_k, \ldots, b_{k+\nu-1}}] \qquad (\nu = 0, 1, \ldots, l-1)$$

genau die sämtlichen zu ξ äquivalenten reduzierten quadratischen Irrationalitäten.

Sei nun $C=\theta(\xi)\in\mathscr{C}(D)$ mit einer quadratischen Irrationalität ξ der Diskriminante D,

$$\xi=[b_0, b_1, \ldots]=[b_0, \ldots, b_{k-1}, \overline{b_k, \ldots, b_{k+l-1}}]$$

mit $l=\lambda(\xi)$ wie oben, und sei für alle $\nu\geqslant 0$

$$\xi_\nu=[b_\nu, b_{\nu+1}, \ldots]=\frac{P_\nu+\sqrt{D}}{2Q_\nu}$$

mit $P_\nu\in\mathbf{Z}$, $Q_\nu\in\mathbf{N}$. Dann gelten für alle $\nu\geqslant 0$ die Rekursionsformeln

$$b_\nu=[\xi_\nu], \qquad P_{\nu+1}=2b_\nu Q_\nu-P_\nu, \quad Q_{\nu+1}=\frac{D-P_{\nu+1}^2}{4Q_\nu};$$

sind $0\leqslant m<n$ minimal mit $Q_m=Q_n$, so folgt $m=k$, $n=k+l-1$, die Ideale $\theta(\xi_\nu)$ $(k\leqslant\nu<k+l)$ sind genau die reduzierten Ideale von C, und $Q_\nu=\mathscr{N}\theta(\xi_\nu)$ sind ihre Normen; ich setze

$$\mathscr{Q}^*(\xi)=\{Q_\nu \mid k\leqslant\nu<k+l\}.$$

Insbesondere ist dann $\mathscr{Q}^*(\omega_D)$ die Menge der Normen der reduzierten Hauptideale von $\mathscr{R}_D$.

2. Eine Klassenzahlabschätzung

Für eine Diskriminante D sei $\mathscr{Q}(D)$ die Menge der Normen primitiver Hauptideale von $\mathscr{R}_D$. Für eine endliche Menge $\mathscr{P}=\{p_1, \ldots, p_n\}$ von (paarweise verschiedenen) Primzahlen $p_1, \ldots, p_n$ und eine reelle Zahl $A>0$ sei $\mathscr{P}(A)$ die Menge aller Potenzprodukte $q=\prod_{i=1}^n p_i^{a_i}$ $(a_i\geqslant 0)$ mit $q\leqslant A$, und

$$\delta_{\mathscr{P}}(A)=\sum_{q\in\mathscr{P}(A)} 2^{\omega(q)};$$

dabei ist $\omega(q)$ die Anzahl der verschiedenen Primteiler von q. Mit diesen Bezeichnungen gilt:

Satz 1. *Sei D eine Diskriminante, $A>0$ und $\mathscr{P}$ eine endliche Menge von Primzahlen, so daß gilt:*

1. $(D/p)=1$ *für alle* $p\in\mathscr{P}$;
2. $\mathscr{P}(A)\cap\mathscr{Q}(D)=\{1\}$.

Dann folgt

$$h_D \geqslant \delta_{\mathscr{P}}(\sqrt{A});$$

im Falle $\#\mathscr{P}=1$, $\mathscr{P}=\{p\}$ *gilt etwas schärfer*

$$h_D \geqslant 1+\left[\frac{\log A}{\log p}\right].$$

Beweis. Sei zunächst $\mathscr{P}=\{p\}$, P ein Primteiler von p in $\mathscr{R}_D$ und $f\in\mathbf{N}$ maximal mit $p^f\leqslant A$, also $f=[\log A/\log p]$; dann sind die $\mathscr{R}_D$-Ideale P^a mit $0\leqslant a\leqslant f$ paarweise inäquivalent und daher $h_D\geqslant 1+f$.

Im allgemeinen Fall sei $\mathscr{P}=\{p_1, ..., p_n\}$, τ der erzeugende Automorphismus von $Q(\sqrt{D})$ und $p_i\mathscr{R}_D=P_i\cdot P_i^\tau$ die Primidealzerlegung in $\mathscr{R}_D$. Dann genügt es, zu zeigen: Die Ideale

$$Q=P_1^{\varepsilon_1 a_1}\cdot \quad\cdots\quad \cdot P_n^{\varepsilon_n a_n}\lhd\mathscr{R}_D$$

mit $\varepsilon_i\in\{1,\tau\}$, $a_i\geqslant 0$, so daß

$$\prod_{i=1}^n p_i^{a_i}\leqslant\sqrt{A}$$

sind paarweise inäquivalent.

Angenommen, es sei

$$P_1^{\varepsilon_1 a_1}\cdot \quad\cdots\quad \cdot P_n^{\varepsilon_n a_n}\sim P_1^{\varepsilon_1' a_1'}\cdot \quad\cdots\quad \cdot P_n^{\varepsilon_n' a_n'}$$

mit ε_i, $\varepsilon_i'\in\{1,\tau\}$, $a_i\geqslant 0$, $a_i'\geqslant 0$, so daß $\prod_{i=1}^n p_i^{a_i}\leqslant\sqrt{A}$, $\prod_{i=1}^n p_i^{a_i'}\leqslant\sqrt{A}$. Dann kann ich o. E. $\varepsilon_i\neq\varepsilon_i'$ für alle $i\in\{1, ..., n\}$ annehmen und erhalte

$$\begin{aligned}p_1^{a_1'}\cdot \quad\cdots\quad \cdot p_n^{a_n'}\cdot\mathscr{R}_D&=P_1^{(\varepsilon_1+\varepsilon_1')a_n'}\cdot \quad\cdots\quad \cdot P_n^{(\varepsilon_n+\varepsilon_n')a_n'}\\&\sim P_1^{\varepsilon_1(a_1+a_1')}\cdot \quad\cdots\quad \cdot P_n^{\varepsilon_n(a_n+a_n')}=Q,\end{aligned}$$

also

$$Q\sim 1,\qquad \mathscr{N}(Q)=\prod_{i=1}^n p_i^{a_i+a_i'}\leqslant A,$$

ein Widerspruch! ∎

In der Literatur wurde bisher ausschließlich der Fall $\#\mathscr{P}=1$ im Falle reell-quadratischer Hauptordnungen behandelt [5, 6, 12, 2, 9]. Eine geeignete Konstante A erhält man dabei entweder aus der Kettenbruchentwicklung von ω_D wie in [6, 1, 2, 9] oder aus der Kenntnis einer nichttrivialen Einheit von $\mathscr{R}_D$ mit Hilfe eines Lemmas vom Davenport-

Ankeny–Hasse'schen Typus [5, 17, 12, 13]. Ich gebe nun zunächst eine in der Allgemeinheit der vorliegenden Arbeit gültige Variante dieses Lemmas.

LEMMA 1. *Sei $D>0$ eine Diskriminante, $\varepsilon>1$ eine Einheit von $\mathcal{R}_D$, $\varepsilon=(T+U\sqrt{D})/2$ mit $T, U\in\mathbf{N}$, und $m\in\mathcal{Q}(D)$, $m>1$. Dann folgt*

$$m\geqslant\begin{cases}(T-2)/U^2, & \text{falls } \mathcal{N}(\varepsilon)=+1,\\ T/U^2, & \text{falls } \mathcal{N}(\varepsilon)=-1.\end{cases}$$

Beweis. Sei $m=\mathcal{N}(\mathcal{J})$ mit einem primitiven Hauptideal $\mathcal{J}\neq(1)$ von $\mathcal{R}_D$. Setze ich $\mathcal{J}=(x+y\sqrt{D}/2)$ mit $x, y\in\mathbf{N}$, $x\equiv Dy \bmod 2$, so ist notwendig $(x, y)\mid(2, D)$, also $y>0$ und ich nehme y minimal an. Wegen

$$\frac{x+y\sqrt{D}}{2}\cdot\varepsilon'=\frac{1}{2}\cdot\left(\frac{xT-yUD}{2}+\frac{yT-xU}{2}\cdot\sqrt{D}\right)$$

folgt

$$\left|\frac{yT-xU}{2}\right|\geqslant y$$

und daraus die Behauptung wie in [5; Sektion 1]. ∎

Mit Hilfe von Satz 1 und Lemma 1 erhält man bereits Verschärfungen aller Klasenzahlabschätzungen aus [5, 12, 9, 2], soferne sie sich nicht auf spezielle Richaud–Degert'sche Typen beziehen; diese werde ich in den Sektionen 3 und 4 mit Hilfe von Kettenbrüchen noch genauer untersuchen.

Um Satz 1 im Falle $\#\mathcal{P}>1$ anzuwenden, benötigt man Kenntnisse über die Größenordnung von $\delta_{\mathcal{P}}(A)$. Dabei ist manchmal das folgende Lemma nützlich:

LEMMA 2. *Sei $\mathcal{P}=\{p_1, ..., p_n\}$ eine endliche Menge (paarweise verschiedener) Primzahlen $p_1, ..., p_n$, $N\geqslant 2$ und $A\geqslant(p_1\cdot\cdots\cdot p_n)^N$; dann folgt*

$$\delta_{\mathcal{P}}(A)\geqslant(2N+1)^n.$$

Beweis. Für $i\in\{0, 1, ..., n\}$ gehören die Zahlen

$$q=p_{\nu_1}^{n_1}\cdot\cdots\cdot p_{\nu_i}^{n_i}$$

mit $1\leqslant\nu_1<\cdots<\nu_i\leqslant n$, $1\leqslant n_i\leqslant N$ zu $\mathcal{P}(A)$ und erfüllen $\omega(q)=i$; daher folgt

$$\delta_{\mathcal{P}}(A)=\sum_{i=0}^{n}\sum_{\substack{q\in\mathcal{P}(A)\\ \omega(q)=i}}2^i\geqslant\sum_{i=0}^{n}2^i\cdot\binom{n}{i}\cdot N^i=(1+2N)^n. \quad ∎$$

Für imaginärquadratische Ordnungen erhält man aus Satz 1 unmittelbar

SATZ 2. *$D<0$ sei eine Diskriminante, $\mathscr{P}$ eine endliche Menge von Primzahlen p mit $p \leqslant |D|/4$ und $(D/p)=1$; dann folgt*

$$h_D \geqslant \delta_{\mathscr{P}}(\tfrac{1}{2}\cdot\sqrt{|D|}).$$

Beweis. Sei $q \in \mathscr{P}(|D|/4)$, also $q \leqslant |D|/4$; dann folgt im Falle $D \equiv 1 \bmod 4$

$$q<\frac{1-D}{4},$$

also $q \notin \mathscr{Q}(D)$; im Falle $D \equiv 0 \bmod 4$ folgt wegen $(D, q)=1$

$$q<\frac{-D}{4},$$

also ebenfalls $q \notin \mathscr{Q}(D)$. Daher ist

$$\mathscr{P}\left(\frac{|D|}{4}\right) \cap \mathscr{Q}(D)=\{1\},$$

und die Behauptung folgt aus Satz 1. ∎

BEISPIEL. Seien $a, c, r \in \mathbf{N}$ und $a^N \geqslant c>4$, $4a+r^2<ca^N$, $(a, r)=1$, und $a=p_1 \cdot \cdots \cdot p_n$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_n$. Sei

$$D=-ca^{2N}+r^2$$

eine Diskriminante. Dann folgt $\frac{1}{2}\cdot\sqrt{|D|} \geqslant a^N$ und daher nach Satz 2 und Lemma 2

$$h_D \geqslant (2N+1)^n.$$

3. DISKRIMINANTEN VOM *R-D*-TYP

DEFINITION. Eine Diskriminante $D>0$ heiße *vom R-D-Typ,* wenn entweder $D=n^2+r \equiv 1 \bmod 4$ mit $r \mid 4n$ oder $D=4D'$ und $D'=n^2+r$ mit $r \mid 4n$.

Ich gebe nun für Diskriminanten D vom *R-D*-Typ die Kettenbruchentwicklung von ω_D an und verwende dabei die Bezeichnungen von Sektion 1. Einige dieser Kettenbruchentwicklungen findet man in [6], einige (wenn auch in anderer Terminologie) in [7]; sie sind aber alle leicht direkt nachzurechnen.

A. $D \equiv 1 \bmod 4$, $\omega_D = \frac{1}{2}\cdot(1+\sqrt{D})$.

1. $D = 4a^2 + r$, $r \equiv 1 \bmod 4$, $r \geqslant 1$, $r \mid a$:

$$\omega_D = \left[a, \overline{1, 1, \frac{2a}{r} - 1, 1, 1, 2a-1}\right],$$

$$\mathcal{Q}^*(\omega_D) = \left\{1, a + \frac{r-1}{4}, a - \frac{r-1}{4}, r\right\}.$$

2. $D = 4a^2 - r$, $r \equiv -1 \bmod 4$, $r \geqslant 1$, $r \mid a$:

$$\omega_D = \left[a, \overline{2, \frac{2a}{r} - 1, 2, 2a-1}\right],$$

$$\mathcal{Q}^*(\omega_D) = \left\{1, a - \frac{r+1}{4}, r\right\}.$$

3. $D = n^2 + 4r$, $n \equiv 1 \bmod 2$, $r \geqslant 1$, $r \mid n$:

$$\omega_D = \left[\frac{n+1}{2}, \overline{\frac{n}{r}, n}\right],$$

$$\mathcal{Q}^*(\omega_D) = \{1, r\}.$$

4. $D = n^2 - 4r$, $n \equiv 1 \bmod 2$, $1 \leqslant r < n$, $r \mid n$:

$$\omega_D = \left[\frac{n-1}{2}, \overline{1, \frac{n}{r} - 2, 1, n-2}\right],$$

$$\mathcal{Q}^*(\omega_D) = \{1, n-r-1, r\}.$$

B. $D = 4D'$, $D' = n^2 + r$ mit $n \geqslant 3$, $r \mid 4n$, $1 \leqslant r < 4n$; $\omega_D = \sqrt{D'}$.

1. $r \mid 2n$:

$$\omega_D = \left[n, \overline{\frac{2n}{r}, 2n}\right],$$

$$\mathcal{Q}^*(\omega_D) = \{1, r\}.$$

2. $r \nmid 2n$, $2 \mid n$:

$$\omega_D = \left[n, \overline{\frac{4n-r}{2r}, 1, 1, \frac{n}{2} - 1, 1, 1, \frac{4n-r}{2r}, 2n}\right],$$

$$\mathcal{Q}^*(\omega_D) = \left\{1, r, n+1-\frac{r}{4}, n-1+\frac{r}{4}, 4\right\}.$$

3. $r \nmid 2n$, $2 \nmid n$:

$$\omega_D = \left[n, \overline{\frac{4n-r}{2r}, 1, 1, \frac{n-1}{2}, \frac{8n}{r}, \frac{n-1}{2}, 1, 1, \frac{4n-r}{2r}, 2n} \right],$$

$$\mathcal{Q}^*(\omega_D) = \left\{ 1, r, n+1-\frac{r}{4}, n-1+\frac{r}{4}, 4, \frac{r}{4} \right\}.$$

C. $D = 4D'$, $D' = n^2 - r$ mit $n \geqslant 3$, $r \mid 4n$, $1 \leqslant r < 2n-1$; $\omega_D = \sqrt{D'}$.

1. $r < n$, $r \mid 2n$:

$$\omega_D = \left[n-1, \overline{1, \frac{2n}{r} - 2, 1, 2n-2} \right],$$

$$\mathcal{Q}^*(\omega_D) = \{1, 2n-r-1, r\}.$$

2. $r < n$, $r \nmid 2n$, $2 \mid n$:

$$\omega_D = \left[n-1, \overline{1, \frac{4n-3r}{2r}, 2, \frac{n}{2} - 1, 2, \frac{4n-3r}{2r}, 1, 2n-2} \right],$$

$$\mathcal{Q}^*(\omega_D) = \left\{ 1, 2n-r-1, r, n-1-\frac{r}{4}, 4 \right\}.$$

3. $r < n$, $r \nmid 2n$, $2 \nmid n$:

$$\omega_D = \left[n-1, \overline{1, \frac{4n-3r}{2r}, 2, \frac{n-3}{2}, 1, \frac{8n}{r} - 2, 1, \frac{n-3}{2}, 2, \frac{4n-3r}{2r}, 1, 2n-2} \right],$$

$$\mathcal{Q}^*(\omega_D) = \left\{ 1, 2n-r-1, r, n-1-\frac{r}{4}, 4, 2n-4-\frac{r}{4}, \frac{r}{4} \right\}.$$

4. $r = n$:

$$\omega_D = [n-1, \overline{2, 2n-2}],$$

$$\mathcal{Q}^*(\omega_D) = \{1, n-1\}.$$

5. $r = 4n/3$, $2 \mid n$:

$$\omega_D = \left[n-1, \overline{3, \frac{n}{2} - 1, 3, 2n-2} \right],$$

$$\mathcal{Q}^*(\omega_D) = \{1, r-1, 4\}.$$

6. $r=4n/3,\ 2\nmid n$:

$$\omega_D=\left[n-1, \overline{3, \frac{n-3}{2}, 1, \frac{n-3}{2}, 3, 2n-2}\right],$$

$$\mathcal{Q}^*(\omega_D)=\left\{1, r-1, 4, \frac{5n}{3}-4\right\}.$$

Ist D eine Diskriminante vom R-D-Typ, so kennt man alle Normen reduzierter Hauptideale und damit alle primitiven Lösungen der diophantischen Gleichung

$$\begin{cases} x^2-Dy^2=\pm 4m, & \text{falls} \quad D\equiv 1 \bmod 4,\ 1\leqslant m<\frac{1}{2}\sqrt{D}, \\ x^2-D'y^2=\pm m, & \text{falls} \quad D=4D',\ 1\leqslant m<\sqrt{D'}. \end{cases}$$

Daraus erhält man einen einfachen Beweis und eine Verallgemeinerung der Sätze von Yokoi [16, Theorem 2] und Mollin [13, Theorem 1.2].

Gemeinsam mit Satz 1 liefert die Kenntnis von $\mathcal{Q}^*(\omega_D)$ Klassenzahlabschätzungen wie folgt:

Satz 3. *Seien $a, c, r\in \mathbf{Z}$, $a\geqslant 2$, $c\geqslant 1$, $\mathcal{P}$ die Menge aller ungeraden Primteiler von a und $(r/p)=1$ für alle $p\in\mathcal{P}$.*

Sei $D>0$ eine Diskriminante von einem der folgenden Typen:

(a) *$D=4a^2c^2+r\equiv 1 \bmod 4$ mit $r\mid c$ und $r\not\equiv 1 \bmod p$ für alle $p\in\mathcal{P}$;*

(b) *$D=a^2c^2+4r\equiv 1 \bmod 4$ mit $r\mid c$, und $r\not\equiv 1 \bmod p$ für alle $p\in\mathcal{P}$, falls $r<0$.*

(c) *$D=4D'$ mit $D'=a^2c^2+r$, $r\mid 2c$, $|r|<ac$, und $r\not\equiv 1 \bmod p$ für alle $p\in\mathcal{P}$, falls $r<0$.*

Dann folgt

$$h_D\geqslant \delta_{\mathcal{P}}\left(\sqrt[4]{\frac{D}{4}}\right).$$

Beweis. Wegen $\mathcal{P}(\frac{1}{2}\cdot\sqrt{D})\cap\mathcal{Q}(D)\subset\mathcal{Q}^*(\omega_D)$ folgt die Behauptung aus Satz 1 und der expliziten Kenntnis von $\mathcal{Q}^*(\omega_D)$. ∎

Für die speziellen Diskriminanten $D=n^2+r$ mit $r\in\{1, 4\}$ erhalte ich im nächsten Paragraphen noch schärfere Resultate.

4. Diskriminanten von speziellem R-D-Typ

Satz 4. *Sei $D>0$ eine Diskriminante, $a\geqslant 2$. Dann gilt:*

$$h_D \geqslant \begin{cases} d(a)-1, & \textit{falls} \quad D=4a^2+1; \\ d(a)-1, & \textit{falls} \quad D=a^2+4\equiv 1 \bmod 4; \\ 2\cdot d(a)-2, & \textit{falls} \quad D=4D' \textit{ mit } D'=a^2+1\equiv 2 \bmod 4. \end{cases}$$

Dabei ist $d(a)$ die Anzahl der Teiler von a.

Beweis. (a) $D=4a^2+1$: Für $1 \leqslant c \mid a$ sei

$$\xi_c = \frac{1+2c+\sqrt{D}}{2c};$$

ξ_c ist eine quadratische Irrationalität mit Diskriminante D und hat die Kettenbruchentwicklung

$$\xi_c = \left[1+\frac{a}{c}, \overline{2c-1, 1, \frac{2a}{c}-1}\right];$$

daher sind die Klassen $\theta(\xi_c) \in \mathscr{C}(D)$ für $1 < c \mid a$ paarweise verschieden, und es folgt $h_D \geqslant d(a)-1$.

(b) $D=a^2+4\equiv 1 \bmod 4$: Für $c \mid a$, $1<c<a$ sei

$$\xi_c = \frac{2+c+\sqrt{D}}{2c};$$

ξ_c is eine quadratische Irrationalität mit Diskriminante D und hat die Kettenbruchentwicklung

$$\xi_c = \left[\frac{a+c}{2c}, \overline{c-1, 1, \frac{a}{c}-1}\right];$$

daher sind die Klassen $\theta(\xi_c) \in \mathscr{C}(D)$ für $c \mid a$, $1<c<a$ pairweise verschieden und erfüllen $\theta(\xi_c) \neq 1$; daraus folgt $h_D \geqslant d(a)-1$.

(c) $D=4D'$ mit $D'=a^2+1\equiv 2 \bmod 4$: Für $1<c \mid a$ sei

$$\xi_c^{\pm} = \frac{\pm(1+c)+\sqrt{D'}}{c};$$

die Zahlen $\xi_c^{\pm}$ sind quadratische Irrationalitäten mit Diskriminante D und den Kettenbruchentwicklungen

$$\xi_c^{+} = \left[\frac{a}{c}+1, \overline{c-1, 1, \frac{2a}{c}-1}\right];$$

$$\xi_c^{-} = \left[\frac{a}{c}-2, \overline{1, c-1, \frac{2a}{c}}\right].$$

Daher sind die Klassen $\theta(\xi_c^+)$, $\theta(\xi_c^-)$ für $c \mid a$, $1 < c < a$, $\theta(\xi_a^+) = \theta(\xi_a^-)$ und $1 = \theta(\sqrt{D'})$ paarweise verschieden, und es folgt $h_D \geqslant 2d(a-2)$. ∎

LITARATUR

1. T. AZUHATA, On the fundamental units and the class numbers of real quadratic fields, *Nagoya Math. J.* **95** (1984), 125–135.
2. T. AZUHATA, On the fundamental units and the class numbers of real quadratic fields, II, *Tokyo J. Math.* **10** (1987), 259–270.
3. G. DEGERT, Über die Bestimmung der Grundeinheit gewisser reellquadratischer Zahlkörper, *Abh. Math. Sem. Univ. Hamburg* **22** (1958), 92–97.
4. P. G. L. DIRICHLET, "Vorlesungen über Zahlentheorie," Braunschweig, 1893; Chelsea Reprint, 1968.
5. H. HASSE, Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper, *Elem. Math.* **20** (1965), 49–59.
6. M. D. HENDY, Applications of a continued fraction algorithm to some class number problems, *Math. Comp.* **28** (1974), 267–277.
7. E. L. INCE, Cycles of reduced ideals in quadratic fields, *in* "Math. Tables," Vol. IV, Cambridge, 1968.
8. B. W. JONES, "The Arithmetic Theory of Quadratic Forms," Carus Mathematical Monographs, Vol. 10, Wiley, New York, 1967.
9. S. LOUBOUTIN, Continued fractions and real quadratic fields, *J. Number Theory* **30** (1988), 167–176.
10. R. A. MOLLIN, A survey of class numbers of quadratic fields in relation to integer solutions of diophantine equations, *Berichte Math. -Stat. Sekt. Forschungszentrum Graz* **272** (1986), 37–48.
11. R. A. MOLLIN, Diophantine equations and class numbers, *J. Number Theory* **24** (1986), 7–19.
12. R. A. MOLLIN, Lower bounds for class numbers of real quadratic fields, *Proc. Amer. Math. Soc.* **96** (1986), 545–550.
13. R. A. MOLLIN, On the insolubility of a class of Diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud–Degert type, *Nagoya Math. J.* **105** (1987), 39–47.
14. O. PERRON, "Die Lehre von den Kettenbrüchen," Bd. 1, Teubner, 1954.
15. Y. YAMAMOTO, Real quadratic number fields with large fundamental units, *Osaka J. Math.* **8** (1971), 261–270.
16. H. YOKOI, On the diophantine equation $x^2 - py^2 = \pm 4q$ and the class number of real subfields of a cyclotomic field, *Nagoya Math. J.* **91** (1983), 151–161.
17. H. YOKOI, Class number one problem for certain kind of real quadratic fields, "Proceedings, Int. Conf. on Class Numbers and Fundamental Units," Katata, 1986.
18. H. YOKOI, Some relations among new invariants of prime number p congruent to 1 mod 4, *Adv. Stud. Pure Math.* **13** (1988), 493–501.